

title, or the disclosure of information to Congress or the Comptroller General of the United States.

(Added Pub. L. 107-296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2267.)

APPLICABILITY OF SECTION

This section not to apply while subchapter III of this chapter is in effect, see section 3549 of this title.

SUBCHAPTER III—INFORMATION SECURITY

§ 3541. Purposes

The purposes of this subchapter are to—

- (1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;
- (2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;
- (3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;
- (4) provide a mechanism for improved oversight of Federal agency information security programs;
- (5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and
- (6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

(Added Pub. L. 107-347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2946.)

EFFECTIVE DATE

Pub. L. 107-347, title IV, §402(b), Dec. 17, 2002, 116 Stat. 2962, provided that: “Title III [see Short Title of 2002 Amendments note set out under section 101 of this title] and this title [enacting provisions set out as a note under section 3601 of this title] shall take effect on the date of enactment of this Act [Dec. 17, 2002].”

§ 3542. Definitions

(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

- (1) The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
 - (A) integrity, which means guarding against improper information modification

or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

(2)(A) The term “national security system” means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) the function, operation, or use of which—

- (I) involves intelligence activities;
- (II) involves cryptologic activities related to national security;
- (III) involves command and control of military forces;
- (IV) involves equipment that is an integral part of a weapon or weapons system; or
- (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(3) The term “information technology” has the meaning given that term in section 11101 of title 40.

(Added Pub. L. 107-347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2947.)

§ 3543. Authority and functions of the Director

(a) IN GENERAL.—The Director shall oversee agency information security policies and practices, including—

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

(A) information collected or maintained by or on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(3) coordinating the development of standards and guidelines under section 20 of the Na-